



$$\Rightarrow 11 \mid (2^{340} - 1)$$

مناسبة ثانية  
بأن 2 و 31 أوليان متباينين

$$2^{30} \equiv 1 \pmod{31}$$

$$\begin{aligned} 2^{340} &= (2^{30})^{11} \cdot 2^{10} \equiv 2^{10} \pmod{31} \\ &\equiv (2^5)^2 \pmod{31} \equiv 1 \pmod{31} \end{aligned}$$

$$2^{340} \equiv 1 \pmod{31}$$

$$\Rightarrow 31 \mid (2^{340} - 1)$$

$$31 \cdot 11 \mid (2^{340} - 1)$$

$$\Rightarrow 341 \mid (2^{340} - 1)$$

فإن 11 و 31 أوليان متباينين وبالتالي فإن

$\Rightarrow$

$$2^{340} \equiv 1 \pmod{341}$$

لذلك يمكن أن تكون مرتبة فرما لـ 2 هي 341 في الحالة العامة

$$2^{340} \equiv 1 \pmod{341}$$

341 ليس أولياً

\* أي إذا كن

$$a^{m-1} \equiv 1 \pmod{m}$$

وبالتالي ليس بالضرورة أن يكون  $m$  أولياً



\* الأعداد من النوع

$$2^n \equiv 2 \pmod{n}$$

مستقيمات أولية وهي مجموعة غير متناهية

برهان سؤال امتحان

بين أن إذا كان  $d(a, 35) = 1$  فإن  $d(a, 5) = d(a, 7) = 1$  فثبت أن

$$a^{12} \equiv 1 \pmod{35}$$

$$a^4 \equiv 1 \pmod{5} \Rightarrow a^{12} \equiv 1 \pmod{5}$$

$$a^6 \equiv 1 \pmod{7} \Rightarrow a^{12} \equiv 1 \pmod{7}$$

5، 7 أوليان متباينين وبالتالي فبما أن 12

إذا كان  $d(a, b, 42) = 1$  فثبت أن

$$(a^6 - b^6) \equiv 0 \pmod{168}$$

$$168 = 3 \cdot 7 \cdot 8$$

$$42 = 2 \cdot 3 \cdot 7$$

$$d(a, b, 42) = 1$$

هذا يعني أن  $a$  مع 3، 7، 8

$$d(a, 3) = d(a, 7) = d(a, 8) = 1$$

$$d(b, 3) = d(b, 7) = d(b, 8) = 1$$

$$a^2 \equiv 1 \pmod{3}$$

$$a^6 \equiv 1 \pmod{7}$$

وبالتالي لا تكفي

$$a^7 \equiv 1 \pmod{8} \text{ لأن } 8 \text{ ليس عدداً أولياً ولا ينطبق}$$

هواييك

علیاً صبره نه حرفاً.

$$d(a, b, 8) = 1$$

$a, b$  لا یکن ان یكون زوجین، ولا یکن اعداداً فردی و الا حرفه زوجی و یساى  $a$  و  $b$  عددان فردیان.

$$a^2 \equiv 1 \pmod{8}$$

$$b^2 \equiv 1 \pmod{8}$$

$$\Rightarrow a^6 \equiv 1 \pmod{8}$$

$$b^6 \equiv 1 \pmod{8}$$

بـطـرحـ صـبـطـواى  
اـتـطـابـقـات

$$(a^6 - b^6) \equiv 0 \pmod{8}$$

$$\Rightarrow 8 \mid (a^6 - b^6)$$

و یساى عدد 3، 7، 8 یسه  $(a^6 - b^6)$

\* صبره نه و یساى سابت الیه  
اذا كان  $P$  عدداً أولياً فإنه

$$(P-1)! \equiv -1 \pmod{P}$$

$$\mathbb{Z}_P \mid (P-1)! + 1 = 0$$

$$(-1) = P-1$$

$$P \mid [(P-1)! + 1]$$

و

$$(P-1)! \equiv (P-1) \pmod{P}$$

$$(P-1)(P-2)! \equiv (P-1) \pmod{P}$$

چان  $(P-1)$  اولی مع العدد الأولی  $P$  و یساى یکن الیه

$$(P-2)! \equiv 1 \pmod{P}$$

و یساى صبره نه



$$1 \equiv -1 \pmod{3}$$

$$2 \equiv -1 \pmod{3}$$

$$A = \mathbb{Z}_p \setminus \{0, \pm 1\}$$

$$A = \{2, 3, \dots, p-2\}$$

$$|A| = p-3 \text{ رتبة المجموعة}$$

عنا  $p$  أولي وباشي طرفه هنا  $p \geq 3$  زوجي

$$a \in A : d(a, p) = 1$$

$$\exists a^* \in A \text{ و } a \cdot a^* \equiv 1 \pmod{p}$$

$$\text{معكوس } p-1 \text{ و } (-1)$$

$$a^* \neq a \pmod{p}$$

$$\text{معكوس } (1) \text{ و } (1)$$

لما هنا حساب الباشي

$$p=13$$

$$A = \{2, 3, 4, 5, 6, 7, 8, 9, 10, 11\}$$

$$4 \cdot (10) \equiv 1 \pmod{13}$$

$$(4^{-1}) = 10$$

عندئذ نتوزع  $a$  الى  $(\frac{p-3}{2})$  زوج بحيث حاصل ضرب اي زوجين متزافين مطابق 1 بالفاصل  $p$  وباشي في المثال

$$2 \cdot 3 \cdot 4 \cdot 5 \cdot 6 \cdot 7 \cdot 8 \cdot 9 \cdot 10 \cdot 11 \equiv 1 \pmod{13}$$

$$2 \cdot 3 \cdot \dots \cdot (p-2) \equiv 1 \pmod{p}$$

بفرد طرفي المتطابق

$$2 \cdot 3 \cdot \dots \cdot (p-2) \cdot (p-1) \equiv (p-1) \pmod{p}$$

$$(p-1)! \equiv -1 \pmod{p}$$

دکتر فبرهنة ولسين

$$(n-1)! \equiv -1 \pmod{n}$$

اذا كان  $n > 2$

فمنذ  $n$  يكون أولي.

البرهان:

واذا لم يكن  $n$  أولياً وباتى له عدد حوّل أي له قاسم مثل  $d$  يقسمه

$$d | n \quad 1 < d < n$$

أي  $1 < d \leq n-1$  ومن ثم  
من جهة أخرى:

$$n | (n-1)! + 1$$

$n$  ومن الطرفين

$$(2) \quad d | ((n-1)! + 1)$$

وباتى

من العلاقتين (1) و (2)

$$d | \{ (n-1)! + 1 - (n-1)! \} = 1$$

وباتى  $d = 1$  وهذا يناقض مع كونه  $n$  ليس أولياً  
وباتى  $n$  أولي.

ملاحظة:

وكيف هي طريقة فبرهنة ولسين ويكبر على النحو الآتي:

يكون  $n$  اذا  $n \geq 2$  أولياً اذا وفقط اذا كان

$$(n-1)! \equiv -1 \pmod{n}$$

ويمكن لهذا المعيار للاعداد الأولية بسبب سرعة تزايد  $n!$  وخاصة عند  $n$  كبيراً

مركباً

نستأن

$$18! \equiv -1 \pmod{437}$$

$$(20)^2 < 437 < (21)^2$$

$$(21)^2 - 437 = 4$$

$$437 = 19 \cdot 23$$



مربعه  
ثبت ان العدد

$$127 \mid [7 \cdot (126!) + 5!]$$

127 عدد أولي حسب ويليس

$$(126)! \equiv -1 \pmod{127}$$

$$\frac{126}{-1} (126)! \equiv -1 \pmod{127}$$

$$(-1) (126)! \equiv -1 \pmod{127}$$

$$(126)! \equiv 1 \pmod{127}$$

$$7 \cdot (126)! \equiv 7 \pmod{127}$$

نطبق نظرية فيرما

$$5! + 7 \cdot (126)! \equiv 7 + 5! \pmod{127}$$

$$\equiv 127 \pmod{127}$$

$$5! + 7 \cdot (126)! \equiv 0 \pmod{127}$$

وبالتالي

$$127 \mid [7 \cdot (126)! + 5!]$$

هذا هو أكثر دليلا على صحة نظرية فيرما

مربعه

اذ كان  $p$  عددا أوليا فهو عدد اولي

$$x^2 \equiv -1 \pmod{p}$$

اذ كان  $p \equiv 1 \pmod{4}$

$$p \equiv 1 \pmod{4}$$

في هذه الحالة يكون ذلك

$$p \equiv 1 \pmod{4}$$

فان

$$x = \left( \frac{-1}{p} \right)$$

$$x^2 \equiv -1 \pmod{p}$$

مثال ۱:

$$5 \equiv -1 \pmod{4} \quad \text{و } p=5$$

$$x = \left(\frac{5-1}{2}\right)! = 2! = 2$$

$$(2)^2 = 4 \equiv -1 \pmod{5}$$

$$x = \left(\frac{13-1}{2}\right)! = 6! = 720 \quad p=13$$

$$(720)^2 \equiv \quad \pmod{13}$$

• • •  
نتیجه همان است